Sindoh MF2000, MF3000, MF4000, N630 Series

Security Target Lite V1.0

This document is a translation of the Security Target written and evaluated in Korean into English.

Document History

Version	Date	Description of change	Remarks
V1.0	2024.10.02	Publication version	

Table of Contents

List of Tables

1. Security Target Overview

This security target is the security target for Sindoh's Sindoh MF2000, MF3000, MF4000, N630 Series (hereinafter referred to as "TOE"). This security target describes the basic information on the identification and operational environment of TOE and the security requirements and assurance requirements provided by TOE.

1.1 Security Target references

This security target can be uniquely identified by the following reference information.

Title	Sindoh MF2000, MF3000, MF4000, N630 Series Security Target Lite
Version	V1.0
Date	October 2, 2024
Author	Sindoh CSD Department

1.2 TOE references

This security target can uniquely identify TOE using the following reference information. TOE can be uniquely identified using the TOE name and TOE version.

TOE name	Sindoh MF2000, MF3000, MF4000, N630 Series
TOE version	V241002_3
Date	October 2, 2024
Developer	Sindoh Co., Ltd.
F/W Package	JUNIPER-R_Pkg_241002_3 (JUNIPER-R_Pkg_241002_3.zip)
Components	JUNIPER-R_CTL JUNIPER-R_241002_3 JUNIPER-R_EGB :15.18.1 JUNIPER-R_UICC :0.0.8 JUNIPER-R_DFC :02.25 JUNIPER-R_BANK :1.10
MFP product model	MF2087, MF3037, MF4063, MF4123, N631, N633

(*The F/W package includes JUNIPER_CTL, JUNIPER_S_EGB, JUNIPER_S_UICC, JUNIPER_S_DFC and JUNIPER_BANK, and is distributed in zip format (e.g. JUNIPER-R_Pkg_241002_3.zip).)

1.3 TOE overview

This section defines TOE Type, TOE Usage and Major Security Features of TOE.

1.3.1 TOE Types

TOE is MFPs (MFPs: Multi-Function Peripherals[1]) that provides basic functions of copy, print, scan, fax and provides security functions of identification and authentication function, access control function, security audit, security management, protecting stored data, self-protection, fax data control, trusted channel.

1.3.2 Purposes of TOE

The TOE operational environment is illustrated in the following figure, and the purposes of TOEs are described in this section.

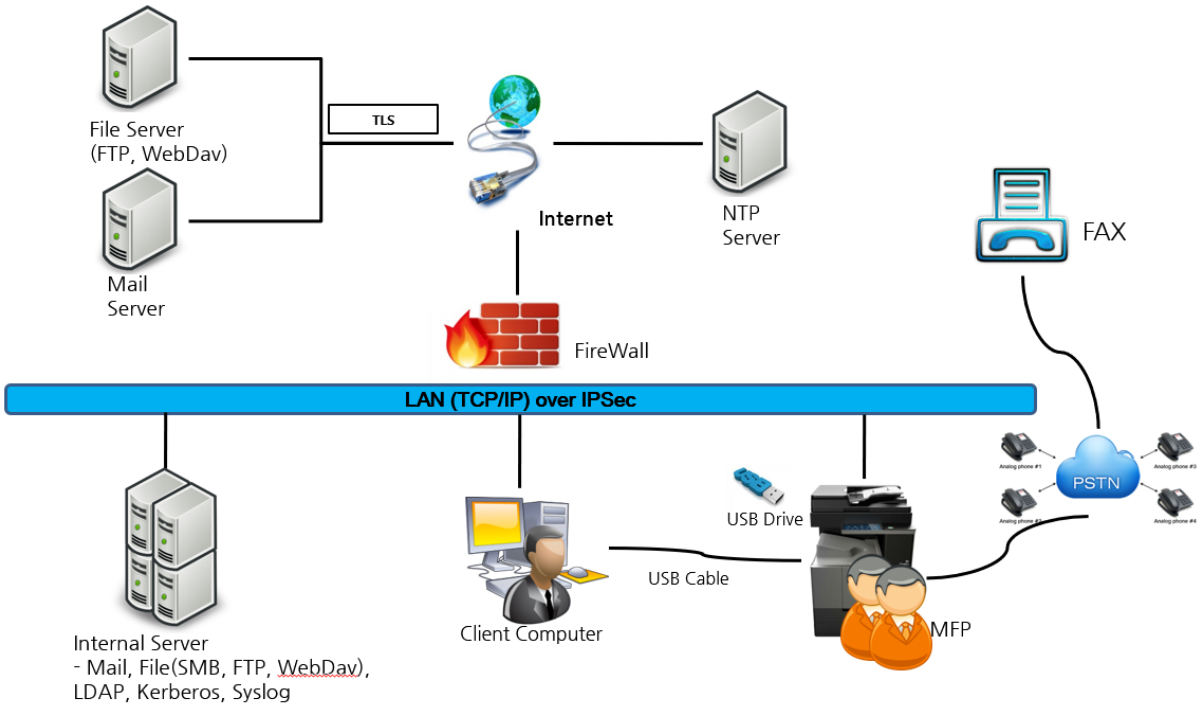

Figure 1. TOE operational environment

TOE is used connected to the local area network (hereinafter referred to as "LAN") as shown in [Figure 1]. Users can operate the TOE using the operation panel or LAN communication. The purposes of TOE (MFPs) and hardware and software other than TOE will be described below.

The purposes of TOE (MFPs) are as follows:

- MFP: The TOE is the MFP. The MFP is connected to LAN, and users can use the operation panel of the MFP and LAN communication to operate the MFP as follows:

[1] MFP: A hardcopy device that fulfills multiple purposes by using multiple functions in different combinations to replace several, single function devices

- Various settings of MFPs
- Copy: Copy a hardcopy document to another hardcopy document (only black and white)
- Print: Print out an electronic document as a hardcopy document (it is possible to use the LAN and USB to print out)
- Scan: Convert a hardcopy document into an electronic file (it is possible to send a scanned image to a remote file server and an e-mail address, and save it in a USB flash drive)
- Fax: Scan a hardcopy document and use PSTN (Public Switched Telephone Network) to send it to a recipient, or print out an image received over PSTN

The following are Non-TOE Hardware devices.

- Client Computer: The computer that performs the role of TOE's client when the TOE is connected to LAN. The user and Administrator can use the Client Computer to operate the MFP remotely. The functions that can be performed remotely using the Client Computer are as follows:
  - Setting up the MFP in various ways by using the web browser installed in the Client Computer
  - Printing and saving documents by using the printer driver installed in the Client Computer
  - Sending a scan command and saving images by using the scanner driver installed in the Client Computer.
- File Server (FTP, WebDAV, SMB): The server for receiving and saving scan data from the TOE.
- Mail Server: The server for sending security warnings or scan data to the administrator
- LDAP Server: The external server that performs identification and authentication of the user (U.USER) entered through LUI using LDAP (Lightweight Directory Access Protocol) or is used to download user address book data.
- Kerberos Server: When using Kerberos authentication to send scan data to an SMB server, it is a server that performs identification and authentication of the user.
- Syslog Server: A server that receives and monitors system events, device status information, and user login history from the TOE.
- NTP Server: A server used to synchronize the TOE's time using NTP.

The following are Non-TOE Software programs.

- Web browser: Provides the communication function between the Client Computer and the MFP. (Chrome web browser 126.0 version or newer, and Microsoft Edge web browser 126.0 version or newer)
- Printer driver: The software installed in the computer to use the TOE Print function. (Sindoh

N630 MF4000 Series PCL6 version 1.23.3.01, Sindoh N630 MF4000 Series PCL5e version 1.23.3.01, Sindoh N630 MF4000 Series PS version 1.23.3.01)

- Scanner driver: The software installed in the computer to use the TOE Scan function. (Juniper-S-RE_usb_scandriver version v1.1.2.0, Juniper-S-RE_network_twain_scandriver version v1.1.2.0, Juniper-S-RE_network_wia_scandriver version v1.0.2.0)

1.3.3 Major Security Features of TOE

The TOE provides the following security functions. The TOE provides identification and authentication function. The administrator uses the browser installed in the Client Computer to manage the security of the TOE over the network, or uses the operation panel of the TOE to perform security management. Normal users can use the TOE functions through the operation panel of the TOE. When the administrator accesses the TOE for security management, TOE identifies and authenticates the administrator so that the authorized administrator can perform security management, and when a user accesses the TOE, TOE identifies and authenticates the user to provide TOE functions only to the authorized user.

The TOE controls access. The TOE denies all accesses to document data except for document owners, and denies accesses to function data except for function data owners. Also, the TOE denies unauthorized access to each basic function according to the basic function access right set up by the administrator. To control external entities accessing the network service provided by the TOE, the TOE uses the IP information or MAC information of external entities to control access.

The TOE provides the security audit function. The TOE saves and manages all internal history of TOE, e.g. the MFP work log, fax log, and audit log. The work log, fax log, and audit log are stored in the database inside the TOE, and only the administrator can view and manage the audit log through the operation panel. Users can view the work log (Print, Scan and Copy history) and the fax log (Fax history).

The TOE provides the Security Management function. The TOE provides various Security Management functions for safe operation of the TOE, such as audit management, user management, IP & MAC filtering function management, and user data repository management, to the administrator. The administrator can use the Security Management functions to decide whether to use each function, and manage security data and information, e.g. safe management/deletion of TSF data and viewing audit records.

The TOE provides the stored data protection function. The TOE provides the function to encrypt the user data repository (SD card or SSD) to protect the user data stored in the TOE, and provides the function to make data recovery impossible when data in the user data repository is deleted by overwriting all areas of the user data repository with ‘0’. The TOE also provides the self-protection function. To demonstrate correct operation of the TSF, the TOE conducts self-tests at a regular intervals during regular operation, and at the request of authorized users. The TOE also provides the function to verify the integrity of TSF data and TSF for authorized users.

The TOE provides the fax data control function. The TOE uses the external interface over PSTN to limit fax data forwarding. Direct data forwarding from the PSTN to another interface is possible only when it is explicitly allowed by the authorized administrative role.

The TOE provides the trusted channel function. The TOE provides trusted channels (IPSec, TLS) to protect user data or TSF data during communication with other external IT entities through the network.

1.4 TOE Description

This section provides information on the physical boundary of the TOE, the manual and the logical boundary of the TOE to provide general information on the security functions that TOE provides to the potential consumers and evaluators of the TOE.

1.4.1 Physical boundary

The physical boundary of the TOE is the MFP comprising the following hardware components.

- Hardware components: DFC Board, Operation Panel Unit, Engine Controller, System Controller Card, Optional Tray, Printer Engine, USB Host CN, Flatbed Engine, SD Card, SSD, DC Power Unit, AC Power Unit, Fax Board

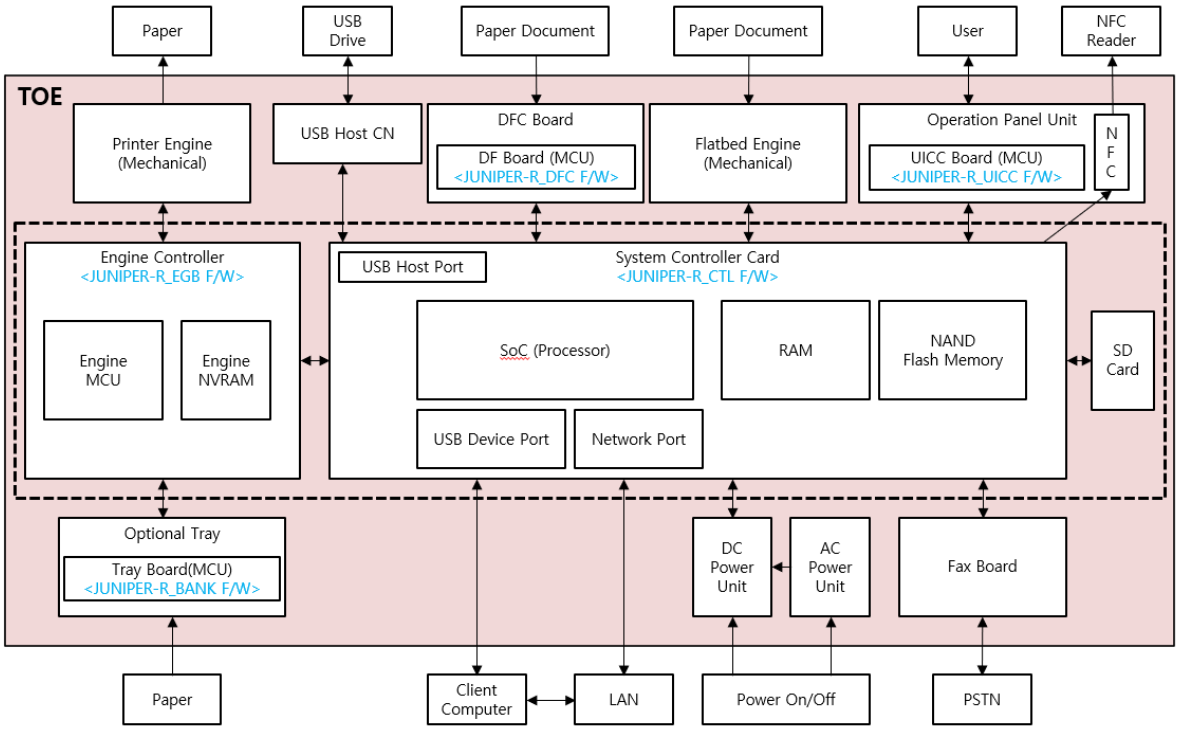

Figure 2. Hardware configuration of the TOE

- Printer Engine: A device that prints out an electronic document as a hardcopy document
- USB Host CN: A connection device for inserting the USB flash drive
- DFC: A board for controlling the document feeder
- Flatbed Engine: Flatbed scanner device
- Operation Panel Unit: A UI touch pad device provided to user so that they can use the TOE
- Engine Controller: A control board for controlling the Printer Engine
- System Controller Card: A control card for controlling the overall functions of the MFP

- SD Card: A user data storage device
- SSD (Solid State Disk): A user data storage device
- Optional Tray: An additional paper feeder
- DC Power Unit: The Power button on the Operation Panel Unit
- AC Power Unit: The power switch connected to the power supply
- Fax Board: A fFax modem for sending and receiving facsimile
- Near Field Communication (NFC): The near field communication device to provide the IP information to the NFC terminal

The firmware included in the TOE is as follows:

[Table 1] Firmware included in the TOE

Classification	N631, N633, MF2087, MF3037, MF4063, MF4123
Controller F/W	JUNIPER-R_CTL :JUNIPER-R_241002_3
Engine Control F/W	JUNIPER-R_EGB :15.18.1
UICC Control F/W	JUNIPER-R_UICC :0.0.8
DFC Control F/W	JUNIPER-R_DFC :02.25
Tray Control F/W	JUNIPER-R_BANK :1.10

As explained above, it is possible to install external programs, such as the printer driver and the scanner driver, in the Client Computer, which is an external IT entity, and use them, and the Client Computer can use IPSec and OpenSSL to form a trusted channel, and safely send driver-related printer data or scan data.

The manuals for using the TOE are as follows:

- Sindoh MF2000, MF3000, MF4000, N630 Series manual V1.1 (N630/MF Series)
- File name: Sindoh MF2000, MF3000, MF4000, N630 Series manual V1.1.pdf

Each firmware, included in the F/W package, which is a TOE element, is installed in the board and included in the machine during production, and the manual in the CD format is packaged with the machine during production, and distributed directly to users.

TOE provides the following 6 MFP models, and the detailed specifications of each model are shown in the table below.

[Table 2] General Specification for MFPs

MFP Product Model		N631	N633	MF2087	MF3037	MF4063	MF4123
Specification							
Copy speed (unit: ppm)		30	48	26	30	42	48
Memory(RAM)		4GB					
Paper Handling		1,000 sheets (500 sheet Tray - 2sets)					
		100 sheets (MPT), 250 sheets (Output Tray)					
Scanner Type		CCDM					
Resolution	Scan	600 dpi					
	Print	Real 1,200 dpi					
Duplex		Standard					
Duplex (Standard)	Document Size	60g/㎡~209g/㎡, 148~431.8mm(length)					
ADF paper loading		90 sheets					
RADF		Standard					
OP Type		10.1 inch Color TFT LCD					
CPU		1.2GHz Quad Core					
FAX module		Standard					
Storage	Default	eMMC: 8GB			eMMC: 8GB SD: 32GB		
	Expansion	SD (1 slot): 64GB SSD (1 slot): 256GB			SSD (1 slot): 256GB		
	MAX	eMMC: 8GB SD: 64GB SSD: 256GB			eMMC: 8GB SD: 32GB SSD: 256GB		
ADF Document Size		Envelope ~ A3/11"x17"					
		Width: 90-297mm , Length: 139.7~431.8mm					
Paper Handling	Tray 1	A5-B4, 5.5"x8.5"~8.5"x14" (500 sheets)					
		(60g/㎡ ~ 220g/ ㎡)					
	Tray 2	A5~A3, 5.5"x9.5"~11"x17" (500 sheets)					
	Manual Tray	A6~A3, 5.5"x 8.5" ~ 11"x 17"					
		(90~297 x 139.7 ~ 431.8)					
		100 Sheets (normal paper), 20 sheets (Thick, OHP), 10 sheets (Envelope)					
		(60g/㎡ ~ 220g/ ㎡, OHP, Envelope)					
	Output Tray	Normal: 60g/㎡ - 250 sheets					
		Think/Special Paper/OHP: 10 sheets					
PS/PCL Control		Standard (PCL 6, PCL5e, PS3)					

* The options listed in [Table 1] are provided by default when the product is shipped.
* SD Cards and SSDs are optional products provided at the user's request, and are used for storing user data.
* eMMC is the area where Controller F/W (JUNIPER-R_CTL) is installed.

1.4.2 Logical Boundary

The basic functions and security functions provided by the MFP are as follows:

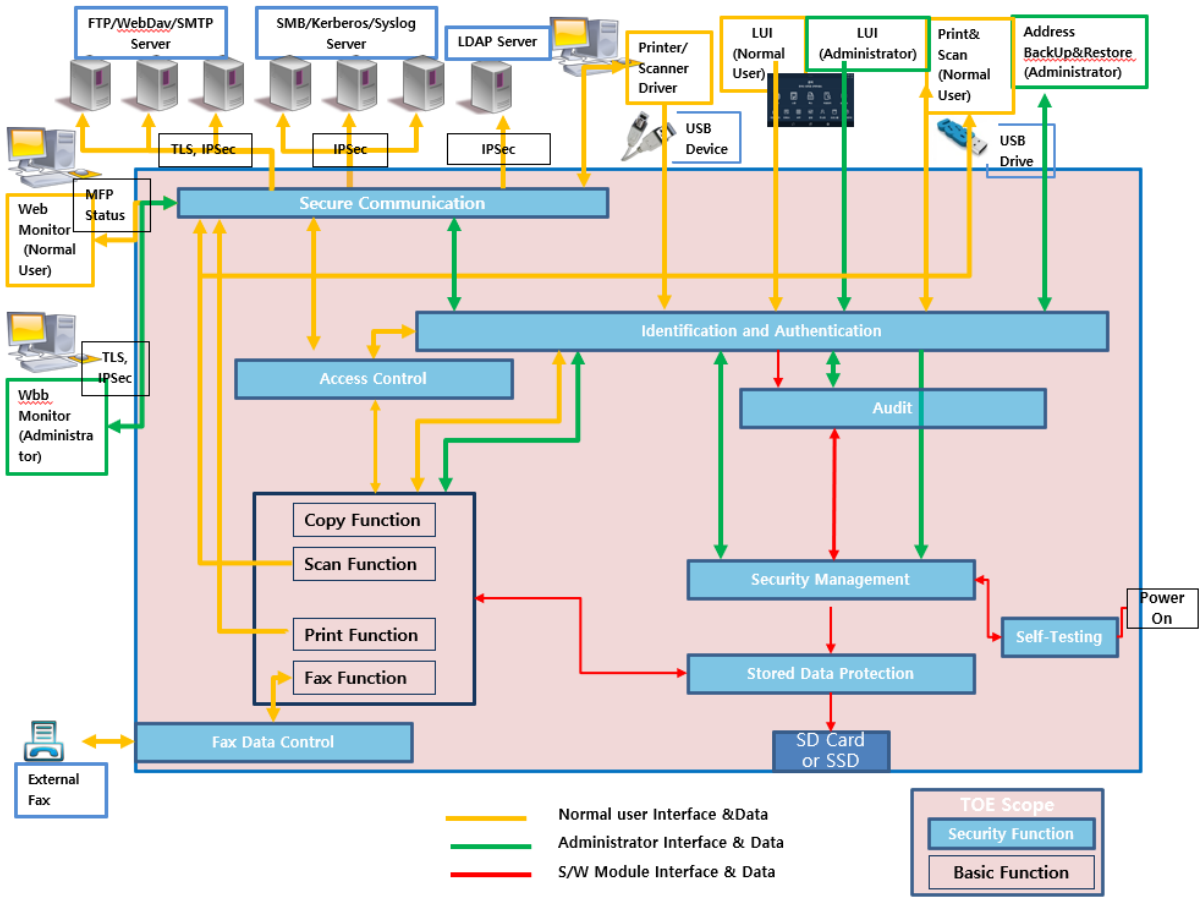

Figure 3. TOE logical boundary

1.4.2.1 Basic functions

The basic functions provided by the MFP are as follows:

- **Print function**

  Producing hardcopy documents from electronic files

- **Scan function**

  Producing electronic files from hardcopy documents, and the operating resolutions can be set at 150dpi, 200dpi, 300dpi, 400dip and, 600dpi.

- **Copy function**

  Duplicating a hardcopy document as a hardcopy document, and the operating resolution is 600dpi.

- **Fax function**

  Scanning a hardcopy document and sending/receiving it over PSTN to print it

1.4.2.2 Security Functions

The security functions provided by the MFP are as follows:

- **Identification and authentication function**

  To be able to access the TOE (using LUI or RUI) and use its functions, users must be identified and authenticated using their ID/password. The identification and authentication data of a user is stored in the database inside the TOE. When a user makes as many consecutive authentication errors as the number of times pre-defined by the administrator, authentication will be limited according to the following authentication failure policy.

  Administrator: Authentication is delayed for a specified amount of time
  Normal user: Authentication is prevented until the administrator allows it again

  Normal user can be identified and authenticated only through LUI, and the administrator can be identified and authenticated through both LUI and RUI.

- **Access control function**

  The TOE controls users who can access the document data generated by the print, scan, fax and copy function based on the user ID, and denies all accesses except for document owners. Also, according to the basic function access right set by the administrator, the rights to execute each basic function are controlled based on user IDs and user roles, and all accesses are denied except for normal users explicitly permitted by the administrator. The TOE provides the function to deny all accesses except for the IPs and MACs allowed by the administrator based on the allowed IPs or MACs set by the administrator.

- **Security audit**

  The TOE stores and manages all internal history of actions occurring in the TOE, such as the MFP work log, fax log, and audit log. These logs can be viewed and managed only by the administrator through the operation panel. The work log (Print, Scan and Copy history) and the fax log (Fax history) can be viewed by the administrator and normal users.

- **Security management**

  The TOE provides security management functions for managing TSF data and security attributes necessary for safely operating the TOE, e.g. management of audit records, user management, IP or MAC filtering function management, and user data repository management. Security management functions can be performed only by the administrator through LUI or RUI.

- **Protecting stored data**

  Data, temporarily stored for printing or fax transmission, or permanently stored by user selection will be stored in the user data repository (SD Card or SSD) installed in the TOE. To protect the user data stored in the data repository, the function to encrypt the data repository is provided. Also, the function to delete the data stored in the data repository is provided to prevent user data in the data repository from being leaked to the outside.

- **Self-protection**

To demonstrate correct operation of the TSF, the TOE conducts self-tests at start-up, periodically during regular operation, and at the request of authorized administrators. It also provides the function to verify the integrity of TSF data and TSF to the authorized administrator to assure that the TSF is operating correctly.

- **Fax data control**

  Unless explicitly permitted by the authorized administrative role, the TOE limits the forwarding of inbound fax data through PSTN to an external interface. Also, except for the fax data, the TOE limits the forwarding of the data received from all external interfaces to all other external interfaces.

- **Trusted channel**

  The TOE provides an encrypted communication function using the following protocol during communication between the TOE and an external IT entity to protect user data or TSF data that is transmitted.

external IT entities	encrypted communication protocol
Client Computer	IPSec, TLS
FTP server	IPSec, TLS
WebDAV server	IPSec, TLS
SMB Server	IPSec
Mail server	IPSec, TLS
LDAP server	IPSec
Kerberos server	IPSec
Syslog server	IPSec

1.5 Terms and definitions

- LUI (Local User Interface)

  The interface for normal users and administrators who directly access, use and manage the digital MFP, and for users who use the operation panel of the digital MFP

- RUI (Remote User Interface)

  The interface for administrators who remotely access, use, and manage the MFP over the web (For normal users, it is possible to check the status information of the machine by not performing identification and authentication.)

- Operation Panel: The MFP's panel that provides LUI for interacting with users to perform functions including security management and viewing the audit log

- Print: Producing hardcopy documents from electronic files

- Scan: Producing electronic files from hardcopy documents

- Copy: Duplicating hardcopy documents

- Fax: Scanning a hardcopy document and sending/receiving it over PSTN to print it

- User data repository: The SD card or SSD (solid-state disk) for storing user data
- TLI (Top Level Index): The identifier for classifying finished products
- User: Authorized users including normal users and administrators who are authorized to use all or part of MFP functions.
- Normal user: An individual user or group user who is authorized by the administrator to use the TOE to perform actions on the user document data
- Individual user: An individual user is authorized by the administrator to use the TOE to perform actions on the user document data.
- Group user: A group user is authorized by the administrator to use the TOE to perform actions on the user document data.
- Administrator: A user with special privilege to manage the whole or parts of the TOE that may influence the TOE security policy
- SMI (Shared-medium Interface): A mechanism for sending or receiving data using the wired and wireless network or non-network electronic method through a communication medium used by several users at the same time
- Box: A storage space inside the machine that can turn the scan data or printer data read by the machine into a file and save it. It is used as a user box and a common box.
- User box: A box that only the user can use through identification and authentication
- Common box: A box that all normal users can share
- Administrator box setting: A setting that only the administrator executes so that box functions can be used

2. Conformance Claim

This chapter describes the common criteria and packages that the security target conforms to

2.1 Conformance to Common Criteria

□ Identification of the common criteria

・Information protection system common criteria part 1: Introduction and general model, 2017. 4, Version 3.1, Revision 5 (CCMB-2017-04-001)

・Information protection system common criteria part 2: security function components, 2017. 4, Version 3.1, Revision 5 (CCMB-2017-04-002)

・Information protection system common criteria part 3: assurance components, 2017. 4, version

3.1 Revision 5 (CCMB-2017-04-003)

□ **Conformance Claim with Common Criteria**

- Extension of common criteria part 2
- Conformance to common criteria part 3

2.2 Conformance to Protection Profiles

There is no protection profile that this security target conforms to.

2.3 Conformance to Packages

This security target conforms to the following assurance package:

□ **Conformance to assurance package EAL2**

2.4 Conformance Claim Rationale

As this security target does not conform to the protection profile, no conformance claim rationale is provided.

3. Security Problem Definition

This section describes threats, security policies of the organization, and assumptions.

The assets handled in the definition of security problems are as follows:

1) User data

   Data generated by users. It does not affect the security functions of the TOE. User data is divided into user document data and user function data.

   User document data (D.DOC) consists of the information contained in user documents. User document data includes the original data, image data, and data stored in the TOE during an operation like spooled data.

   User function data (D.FUNC) is the information on documents or jobs processed by the TOE.

2) TSF Data

   TSF data is the the data generated by the TOE for its operations. It is the data that affects the security operation of the TOE. TSF data is divided into TSF protection data and TSF confidential data.

   TSF protection data (D.PROT) is the data that affects the security operation of the TOE and that is allowed to be disclosed. It is the data that must be protected from the alterations made by users other than the administrator or data owners.

   TSF confidential data (D.CONF) is the data that affects the security operation of the TOE. It is the data that must be protected from the disclosure or alterations made by users other than the administrator or data owners.

3) TOE functions

   TOE functions mean the processing, storing and transmission of the data in the TOE

3.1 Threats

The sources of threats are as follows:

- TOE users who try to access the TOE without the authority to use it
- Authenticated users who try to use TOE functions they are not authorized to use
- Authenticated users who try to access data using unauthorized methods
- Users who cause software errors that may accidentally expose the TOE to unexpected threats

[Table 1] Threats to TOE

Threat	Asset	Description
T.DOC.DIS	D.DOC	User document data may be disclosed to unauthorized users.
T.DOC.ALT	D.DOC	User document data may be altered by unauthorized users.
T.FUNC.ALT	D.FUNC	User function data may be altered unauthorized users.
T.PROT.ALT	D.PROT	TSF protection data may be altered by unauthorized users.
T.CONF.DIS	D.CONF	TSF confidential data may be disclosed to unauthorized users.
T.CONF.ALT	D.CONF	TSF confidential data may be altered by unauthorized users.

3.2 Organizational Security Policies

[Table 2] Organizational Security Policies

Identification	Description
P.USER.AUTHORIZATION	To maintain the safety of the TOE, users must be authorized by the TOE before using the TOE.
P.SOFTWARE.VERIFICATION	To detect alterations of the executable codes in the TSF, the executable codes in the TSF must be self-tested.
P.AUDIT.LOGGING	To trace the responsibility for actions related to security, the TOE must correctly record and maintain security-related events, and make sure that the administrator can appropriately review the audit log.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interface of the TOE, the external interface of the TOE should be managed by the TOE or IT environment.

3.3 Assumptions

[Table 3] Assumptions of TOE

Identification	Description
A.ACCESS.MANAGED	The TOE must be in a physically safe environment, and protected from unauthorized physical accesses.

A.USER.TRAINING	TOE users must know the organizational security policies and procedures, and observe them.
A.ADMIN.TRAINING	The administrator must observe the organizational security policies and procedures, be able to operate according to the TOE manufacturer's guideline and manual, complete operational education, and properly configure and operate the TOE according to the policies and procedures.
A.ADMIN.TRUST	Authorized TOE administrators should not be malicious, and should not abuse their privileges.
A.SERVICES.RELIABLE	The external IT entities that interact with the TOE should be securely managed to ensure the trustworthiness of the information they provide.

4. Security objectives

This security target classifies Security Objectives into Security Objectives for the TOE and Security Objectives for the operational environment. Security Objectives for the TOE are directly covered by the TOE, and the Security Objectives for the operational environment are covered by the IT environment or non-technical/procedural means.

4.1 TOE security objectives

[Table 4] TOE security objectives

Security objectives	Description
O.DOC.NO_DIS	The TOE must protect user document data in the TOE from an unauthorized disclosure
O.DOC.NO_ALT	The TOE must protect user document data in the TOE from unauthorized alterations.
O.FUNC.NO_ALT	The TOE must protect user function data stored in the TOE from unauthorized alterations.
O.PROT.NO_ALT	The TOE must protect TSF protection data from unauthorized alterations.
O.CONF.NO_DIS	The TOE must protect TSF confidential data from unauthorized disclosure.
O.CONF.NO_ALT	The TOE must protect TSF confidential data from unauthorized alterations.
O.USER.AUTHORIZED	The TOE must identify and authenticate users. Also, it must guarantee authority according to the security policies before allowing users to use the TOE.
O.INTERFACE.MANAGED	The TOE must manage external interface operations according to the security policies.
O.SOFTWARE.VERIFIED	The TOE must conduct self-tests for the executable codes in the TSF to detect alterations of the executable codes in the TSF.

O.AUDIT.LOGGED	The TOE must generate and manage audit logs about TOE use and security-related events, and protect the audit logs from unauthorized disclosure and alterations.

4.2 Security Objectives for Operational Environment

The following is a list of Security Objectives that must be handled by technical/procedural means supported by the IT operational environment so that the TOE can provide security functions correctly.

[Table 5] Security Objectives for Operational Environment

Security Objective	Description
OE.INTERFACE.MANAGED	The IT environment must guarantee that the external interfaces of the TOE are protected from unauthorized access.
OE.PHYSICAL.MANAGED	The TOE must be in a physically safe environment, and it must be guaranteed that it is protected from unauthorized physical access.
OE.USER.TRAINED	The TOE owner must guarantee that users know the organizational security policies and procedures, complete the education on observance of policies/procedures, and have the competence required.
OE.ADMIN.TRAINED	The TOE owner must guarantee that the administrator observes the organizational security policies/procedures, has the ability to operate according to the TOE manufacturer's guideline and manual, completes operational education, and correctly configures and operates the TOE according to the policies and procedures.
OE.ADMIN.TRUSTED	The TOE owner must guarantee that the administrators are not malicious, and do not abuse their privileges.
OE.AUDIT.REVIEWED	The TOE owner must guarantee that audit logs are reviewed at appropriate intervals.
OE.USER.AUTHORIZED	The TOE owner must authorize users to use the TOE according to the organizational security policies and procedures.
OE.SERVICES.RELIABLE	Reliable information and responses must be provided to the TOE when using services provided by external IT entity servers.

4.3 Security Objective Rationale

The rationale for security objectives proves that the security objectives are appropriate, and sufficient and necessary for handling security problems.

The rationale for security objectives demonstrates the following:

- Threats, the organizational Security Policies, and assumptions are covered by at least one security objective.
- Each security objective handles at least one threat, organizational security policy and assumptions.

[Table 6] Integrity of Security Objectives

Security Problem Definition / security objectives	T.DOC.DIS	T.DOC.ALT	T.FUNC.ALT	T.PROT.ALT	T.CONF.DIS	T.CONF.ALT	P.USER.AUTHORIZATION	P.SOFTWARE.VERIFICATION	P.AUDIT.LOGGING	P.INTERFACE.MANAGEMENT	A.ACCESS.MANAGED	A.USER.TRAINING	A.ADMIN.TRAINING	A.ADMIN.TRUST	A.SERVICES.RELIABLE
O.DOC.NO_DIS	O														
O.DOC.NO_ALT		O													
O.FUNC.NO_ALT			O												
O.PROT.NO_ALT				O											
O.CONF.NO_DIS					O										
O.CONF.NO_ALT						O									
O.USER.AUTHORIZED	O	O	O	O	O	O	O								
O.INTERFACE.MANAGED										O					
O.SOFTWARE.VERIFIED								O							
O.AUDIT.LOGGED									O						
OE.INTERFACE.MANAGED										O					
OE.PHYSICAL.MANAGED											O				
OE.USER.TRAINED												O			
OE.ADMIN.TRAINED													O		
OE.ADMIN.TRUSTED														O	

OE.AUDIT.REVIEWED									O						
OE.USER.AUTHORIZED	O	O	O	O	O	O	O								
OE.SERVICES.RELIABLE															O

[Table 7] Rationale for Security Objectives

Security problem	Description	Security objective and rationale
T.DOC.DIS	User document data may be disclosed to unauthorized users.	O.DOC.NO_DIS protects user document data from unauthorized disclosure.
		O.USER.AUTHORIZED guarantees that users are identified and authenticated according to the authorization rule.
		OE.USER.AUTHORIZED establishes TOE owners' responsibility for appropriately granting authorization.
T.DOC.ALT	User document data may be altered by unauthorized users.	O.DOC.NO_ALT protects user document data from unauthorized alterations.
		O.USER.AUTHORIZED identifies and authenticates users according to the authorization rule.
		OE.USER.AUTHORIZED establishes TOE owners' responsibility for appropriately granting authorization.
T.FUNC.ALT	User work data may be altered by unauthorized users.	O.FUNC.NO_ALT prevents unauthorized alteration of users' work data.
		O.USER.AUTHORIZED identifies and authenticates users according to the authorization rule.
		OE.USER.AUTHORIZED establishes TOE owners' responsibility for appropriately granting authorization.
T.PROT.ALT	TSF protection data may be altered by unauthorized users.	O.PROT.NO_ALT protects TSF protection data from unauthorized change.
		O.USER.AUTHORIZED identifies and authenticates users according to the authorization rule.
		OE.USER.AUTHORIZED establishes TOE owners' responsibility for appropriately granting authorization.
T.CONF.DIS	TSF confidential data may be disclosed to unauthorized users.	O.CONF.NO_DIS prevents TSF confidential data from unauthorized disclosure.
		O.USER.AUTHORIZED identifies and authenticates users according to the authorization rule.
		OE.USER.AUTHORIZED establishes TOE owners' responsibility for appropriately granting authorization.
T.CONF.ALT	TSF confidential data may be altered by unauthorized users.	O.CONF.NO_ALT prevents TSF confidential data from unauthorized alteration.
		O.USER.AUTHORIZED identifies and authenticates users according to the authorization rule.
		OE.USER.AUTHORIZED establishes TOE owners' responsibility for appropriately granting authorization.
P.USER.AUTHORIZATION	To maintain the safety of the TOE, users must be authorized by the TOE before using the	O.USER.AUTHORIZED identifies and authenticates users according to the authorization rule.

	TOE.	OE.USER.AUTHORIZED establishes TOE owners' responsibility for appropriately granting authorization.
P.SOFTWARE.VERIFICATION	To detect alteration of the executable codes in the TSF, the executable codes in the TSF must be self-tested.	O.SOFTWARE.VERIFIED provides the procedure for self-testing the executable codes in the TSF.
P.AUDIT.LOGGING	To trace the responsibility for actions related to security, the TOE must correctly log and maintain security-related events, and make sure that the administrator appropriately reviews the audit log.	O.AUDIT.LOGGED must generate and manage the audit logs about TOE use and security-related events, and protect the audit logs from unauthorized disclosure and alterations.
		OE.AUDIT.REVIEWED guarantees that the TOE owner reviews the audit logs at appropriate intervals.
P.INTERFACE.MANAGEMENT	To prevent unauthorized use of the external interfaces of the TOE, the TOE or IT environment must protect the external interfaces of the TOE.	O.INTERFACE.MANAGED manages external interface operations according to the TOE security policies.
		OE.INTERFACE.MANAGED builds a protected environment for the external interfaces of the TOE.
A.ACCESS.MANAGED	The TOE must be in a physically safe environment, and protected from unauthorized physical access.	OE.PHYSICAL.MANAGED guarantees a physically safe operational environment for the TOE.
A.USER.TRAINING	The TOE user must know and observe the organizational Security Policies and procedures.	OE.USER.TRAINED guarantees that the TOE owner is responsible for appropriate user education.
A.ADMIN.TRAINING	The administrator must observe the organizational Security Policies and procedures, have the ability to operate according to the TOE manufacturer's guideline and manual, complete operational education, and properly configure and operate the TOE according to the policies and procedures.	OE.ADMIN.TRAINED guarantees that the TOE owner is responsible for appropriate administrator education.
A.ADMIN.TRUST	Authorized TOE administrators should not be malicious, and should not abuse their privileges.	OE.ADMIN.TRUSTED guarantees that the TOE owner maintains a trust relationship with the administrator.
A.SERVICES.RELIABLE	To securely manage external IT entity servers interacting with the TOE, reliable information and responses are provided.	OE.SERVICES.RELIABLE guarantees reliability and security by securely managing external IT entity servers, enabling them to interact with the TOE.

5. Extended Components Definition

Restricted forwarding of data to external interfaces

Overview of the family

This family defines the requirements for the TSF to restrict direct forwarding of information from one external interface to another external interface.

Hierarchical relationship and description of components

FPT_FDI_EXP Restricted forwarding of data to external interfaces	1

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces provides the function to require TSF controlled processing of data received over defined external interfaces before these data are sent out to another external interface. Direct forwarding of data from one external interface to another one requires explicit allowance by an authorized administrative role.

Management: FPT_FDI_EXP.1

The following management functions can be considered in FMT:

a) Definition of the roles that are allowed to perform the management activities

b) Management of the conditions under which direct forwarding can be permitted by an administrative role

c) Revocation of such a permission

Audit: FPT_FDI_EXP.1

No auditable events are foreseen.

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

FPT_FDI_EXP.1.1 The TSF must provide the function to restrict the forwarding of data received from [allocation: external interface list] to [allocation: external interface list] without further processing by the TSF.

Rationale for extension

The TOE provides the function to perform specific checks for and process data received from one external interface before it is allowed to be sent to another external interface. That is, direct forwarding of such data between different external interfaces must be allowed by an authorized role.

If this function comes in a single component, it is possible to specify an attribute that does not allow direct forwarding, and it is required that this job should be allowed only by an authorized role. This function is common to many products, and it has been deemed useful to define it as an extended component.

The Common Criteria defines attribute-based control of user data flow in the FDP class. In this Security Target, however, it is necessary to define the expression about the control of both user data and TSF data flow using administrative control instead of attribute-based control. It is considered inappropriate to use FDP_IFF and FDP_IFC in CC Part II to define it. Accordingly, the authors of this Security Target decided to define an extended component in order to define this function.

As this extended component protects both user data and TSF data, it can be defined in either the FDP class or the FPT class. Since its purpose is to protect the TOE from misuse, the authors believed that it was most appropriate to define it in the FPT class. As it is inappropriate to define it in an existing family, an additional family was defined.

6. Security requirements

This chapter describes the security functional requirements and security assurance requirements that the TOE must satisfy.

The operations (creation rules) applied to security functional requirements are defined as follows:

• Iteration

It is used when diverse operations are applied and a component is repeated several times. The result of the iteration operation is marked by an iteration number in parentheses after the component identifier (i.e. iteration number).

• Assignment

It is used to allocate a certain value to an unspecified parameter (e.g. password length). The result of the assignment operation is marked by square brackets (i.e. [assigned value]).

• Selection

It is used to select one or more options provided by common criteria for information protection systems when describing requirements. The result of the selection operation is *underlined and italicized*.

• Refinement

It is used to further restrict the requirements by adding details to the requirements. The result of the refinement operation is marked in **bold**.

This Security Target defines all subjects, objects, operations, security attributes, and external entities used in security requirements as follows:

Subject (User)

Users are the entities who directly use or interact with the TOE. They are users identified and authenticated by the TOE, and they can be divided into normal users and administrators.

[Table 8] Definitions of Subjects

Identifier		Definition
U.USER		Authorized user
	U.NORMAL	A user authorized to use the TOE to work with user document data
	U.ADMINISTRATOR	A user with a special authority to manage all or part of the TOE. This user can influence the TOE security policies and has a special authority to replace part of the TOE.

Object

An object is a passive entity inside the TOE that includes or receives information when the subjects perform operations. In this security target, the TOE itself is the object. There are three types of objects (user data, TSF data, and function) as shown below.

User data

User data is the data generated by users. It does not affect the security functions of the TOE. User data includes user document data and user function data.

[Table 9] Definitions of User Data

Identifier	Definition
D.DOC	User document data consists of information contained in user documents and includes the original data, image data, and the residual data generated by the MFP during printing.
D.FUNC	User function data means the information on the documents or jobs processed by the TOE.

TSF data

TSF data is the data generated by the TOE for TOE operations, and it influences TOE security operations. TSF data is divided into TSF protection data and TSF confidential data.

[Table 10] Definitions of TSF Data

Identifier	Definition
D.PROT	TSF protection data influences the security operations of the TOE. It is allowed to be disclosed, and it must be protected from alterations made by users other than the administrator or data owners.
D.CONF	TSF confidential data influences the security operations of the TOE. It must be protected from alterations made by users other than the administrator or data owners.

The TSF data used in the TOE is as follows:

[Table 11] TSF data

TSF Data list	TSF confidential data	TSF protection data
Address book		O
User box setting	O	
Work log, fax log		O
Audit log	O	
User ID	O	
User password	O	
User authority (basic function)	O	
Security fax setting	O	
Network setting	O	
Security warning mail setting	O	
Mail server setting	O	

SD Card setting (LUI)	O	
SSD setting (LUI)	O	
Service port	O	
IPSec setting	O	
SNMP setting	O	
Login limit time	O	
Number of login attempts	O	
IP&MAC filtering setting	O	
Administrator connection IP setting	O	
Output authentication setting	O	
Fax data control setting	O	
MFP time setting	O	
Administrator box setting	O	
LDAP setting	O	
ID&Print setting	O	
User counter setting	O	
LDAP Address Book setting	O	
SMB Kerberos Setting	O	
Syslog Setting	O	
IEEE802.1X Setting	O	
Device Certificate Setting (RUI)	O	
CA Certificate Setting (RUI)	O	

TOE functions

TOE functions process, store, and send the data in the TOE.

[Table 12] Basic Functions Provided by TOE

Identifier	Definition
F.PRT	Converts electronic documents into hardcopy documents
F.SCN	Converts hardcopy documents into electronic documents
F.CPY	Duplicates hardcopy documents as hardcopy documents
F.FAX	Converts hardcopy documents into data that can be recognized by the fax (telephone-based document facsimile) and sends it, or prints out the data received by the fax as hardcopy documents

Attributes

It refers to an identification of the functions related to certain data (e.g. security attributes) when data is processed, stored, and sent. The attributes of the TOE can distinguish the functions that are being executed from related SFRs.

[Table 13] attributes

Classification	Description

+PRT	Data related to the print job
+SCN	Data related to the scan job
+CPY	Data related to the copy job
+FAXIN	Data related to the fax receive job
+FAXOUT	Data related to the fax send job

Operations

Operations are specific types of actions performed by the subject with regard to the object. This security target includes 6 types of operations (read, modify, delete, register, backup/restoring the data, and execute).

External entities

[Table 14] Definitions of External Entities

Classification	Description
File server	An external server for storing received fax data or scan data (FTP, WebDav, SMB server)
Mail server	The mail server (SMTP server) used by the TOE to send security warnings
LDAP Server	The external server that performs identification and authentication of the user (U.USER) entered through LUI using LDAP (Lightweight Directory Access Protocol) or is used to download user address book data.
Kerberos Server	When using Kerberos authentication to send scan data to an SMB server, it is a server that performs identification and authentication of the user.
Syslog Server	A server that receives and monitors system events, device status information, and user login history from the TOE.
NTP Server	A server used to synchronize the TOE's time using NTP.
Client PC	The PC with the printer driver or scanner driver installed

6.1 Security functional requirements

The security functional requirements defined in this security target are the related security function components selected from Common Criteria Part 2 to meet the Security Objectives identified in Chapter 4.

6.1.1 Security audit class

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [assignment: send a warning mail to the administrator (U.ADMINISTRATOR)] upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events.

a) Start-up and shutdown of the audit functions

b) All auditable events for the *Not specified* level of audit; and

c) [See the auditable events in [Table 15]]

[Table 15] Auditable events

SFR-related Auditable Events	Details of Auditable Events	Related SFR
Audit log repository saturation	Details of audit log repository saturation	FAU_STG.4
Responses to administrator/user authentication failure	History of responses to authentication failures	FIA_AFL.1
Administrator/user authentication success/failure	Authentication success/failure history	FIA_UAU.1
Data access control setting change	History of data access control setting change	FMT_MSA.1(1)
Basic function access control setting change	History of basic function access control setting change	FMT_MSA.1(2)
Network information flow control setting change	History of network information flow control setting change	FMT_MSA.1(3)
Data access control setting change	History of data access control setting change	FMT_MSA.3(1)
Basic function access control setting change	History of basic function access control setting change	FMT_MSA.3(2)
Network information flow control setting change	History of network information flow control setting change	FMT_MSA.3(3)
Security management result	History of administrator's security management excluding queries	FMT_MTD.1
Self-test result	Self-test result (success/failure)	FPT_TST.1
Session end result	Session end details	FTA_SSL.3
Auditable event related to basic functions	**Details of auditable events**	**Remarks**
Copy	Copy record	Auditable events of basic functions that are not related to SFR
Scan	Scan record	
Fax	Fax send/receive record	
Print	Print record	

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the protection profile/security target, [None]

FAU_GEN.2 User identity association

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs..

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [continuous failures of user authorization (the failure count follows the administrator's setting)] known to indicate a potential security violation;

b) [In case of the audit log repository saturation, and a self-test result error]

FAU_SAR.1 Audit review

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [U.ADMINISTRATOR] with the capability to read [all audit records] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

Dependencies: FAU_SAR.1 audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [Select] of audit data based on [User ID].

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to ***prevent*** unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall ***overwrite the oldest stored audit records*** and [send a warning mail to the administrator (U.ADMINISTRATOR)] if the audit trail is full.

6.1.2 Cryptographic support class

FCS_CKM.1 (1) Cryptographic key generation

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm [Sindoh user data repository cryptographic key generation algorithm] and the specified cryptographic key sizes [256-bits] that meet the following [None].

Application Note: This component describes that generate of cryptographic keys used to encrypt the user data repository.

FCS_CKM.1 (2) Cryptographic key generation

Hierarchical to: No other components

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm [Password Based Key Derivation Function (PBKDF1)] and the specified cryptographic key sizes [256-bits] that meet the following [RFC2898].

Application Note: This component describes that generate of cryptographic keys used for the address book backup/restore function.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data including security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [initialized to 0 (zero)] that meets the following [None].

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data including security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [Cryptographic operations in Table 18] in accordance with the specified cryptographic algorithm [Algorithm in Table 18] and the cryptographic key sizes [Cryptographic key size in Table 18] that meet the following [None].

[Table 16] Cryptographic Operation

Cryptographic Operation	Algorithm	Cryptographic key size
- user data repository encryption - user data repository decryption	AES-CBC	256

- address book backup data encryption - address book backup data decryption	AES-CBC	256

6.1.3 User data protection class

FDP_ACC.1 (1) Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (1) The TSF shall enforce the [Data access control SFP] on [list of operations between subjects and objects handled according to the subject list, object list and SFP in Table 19].

FDP_ACC.1 (2) Subset access control

Hierarchical to: No other components

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 (2) The TSF shall enforce the [basic function access control SFP] on [Table 18].

FDP_ACF.1 (1) Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (1) The TSF shall enforce the [data access control SFP] to objects based on the following: [subjects, objects and the security attributes and operations of subjects and objects in Table 19].

FDP_ACF.1.2 (1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [the following list: Table 19].

[Table 17] Data access control SFP

SFP name	Object	Attributes if objects	Operation	Subject	Security attributes	Control policy
Data access control SFP	D.DOC	+PRT	Delete	U.NORMAL	User ID	Denial excluding document owners
	D.DOC	+PRT	Read	U.NORMAL	User ID	Denial excluding document owners
	D.DOC	+SCN	Delete	U.NORMAL	User ID	Denial excluding document owners
	D.DOC	+SCN	Read	U.NORMAL	User ID	Denial excluding document owners
	D.DOC	+FAXIN +FAXOUT	Delete	U.NORMAL	User ID	Denial excluding document owners
	D.DOC	+FAXIN +FAXOUT	Read	U.NORMAL	User ID	Denial excluding document owners
	D.DOC	+CPY	Read	No restriction on access		
	D.FUNC	+PRT	Delete	U.NORMAL	User	Denial excluding

		+SCN +FAXIN +FAXOUT			ID	function data owners

Application Note: If fax documents are received, the fax job owner is regarded as the administrator.

Application Note: The operation “Read” is described as follows according to the attributes of objects.

Operation	Attributes of objects	Description
Read	+PRT	Forward the hardcopy target to the hardcopy output handler
	+SCN	User document data is delivered through the interface selected by the user.
	+CPY	Forward the hardcopy target to the hardcopy output handler
	+FAXIN +FAXOUT	Uses the hardcopy output handler to deliver the hardcopy target in order to receive fax (+FAXIN), and uses the fax interface to send and receive user document data (+FAXOUT or +FAXIN)

FDP_ACF.1.3 (1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [None]

FDP_ACF.1.4 (1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [None]

FDP_ACF.1 (2) Security attribute based access control

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 (2) The TSF shall enforce the [basic function access control SFP] based on the following: [Table 18].

FDP_ACF.1.2 (2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Table 18]

FDP_ACF.1.3 (2) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [None]

FDP_ACF.1.4 (2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [None]

[Table 18] Basic function access control SFP

SFP name	Object	Attributes of objects	Operation	Subject	Security attribute	Control policy
Basic function access control SFP	F.PRT	Authority	Execution	U.NORMAL	User ID, User role	Denial excluding U.NORMAL explicitly permitted by U.ADMINISTRATOR
	F.SCN					
	F.CPY					

	F.FAX					

FDP_IFC.2 Complete information flow control

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [network information flow control security policy] on [subjects (external IT entities) and information (network packet)] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information flow in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [network information flow control security policy] based on the following types of subject and information security attributes: [list of subjects and information controlled by the following SFP, and the security attributes of subjects and information].

Subjects: External IT

Information: Network Packet

Attributes of Subjects: IP, MAC

Attributes of information: IP, MAC

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [If the subject's IP or MAC is the IP or MAC registered as Allowed in the IP filtering or MAC filtering policy set up by U.ADMINISTRATOR].

FDP_IFF.1.3 The TSF shall enforce [None].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [None].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [None].

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *recovering resources from* the following objects: [SD card and SSD].

Application Note: User data stored in the SD card and SSD is encrypted print data, scan data and fax data.

6.1.4 Identification and authentication class

FIA_AFL.1 (1) Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 authentication

FIA_AFL.1.1 (1) The TSF shall detect when *ranging between [3 and 10], which can be configured by the administrator* unsuccessful authentication attempts occur related to [administrator consecutive authentication failures].

FIA_AFL.1.2 (1) When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [delay authentication by 5~30 minutes].

Application Note: The default number of authentication failures is 5 times during initial installation.

FIA_AFL.1 (2) Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 authentication

FIA_AFL.1.1 (2) The TSF shall detect when *ranging between [3 and 10], which is configurable by the administrator* unsuccessful authentication attempts occur related to [normal user consecutive authentication failures].

FIA_AFL.1.2 (2) When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [delay authentication of normal users].

Application Note: The default number of authentication failures is 5 times during initial installation, and authentication of normal users must be prevented until the administrator changes authentication of the users.

FIA_ATD.1 User attribute definition

Hierarchical to: No other components

Dependencies: No dependencies

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User ID and users' job authority].

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [receiving fax data and using menus unrelated to security (product information, address book, product status information)] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*] to the user while the authentication is in progress

FIA_UID.1 Timing of identification

Hierarchical to: No other components

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [using menus unrelated to security (product information, address book, and product status information)] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

Hierarchical to: No other components

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [User ID and users' job authority]

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [Allocating the security attributes of U.USER to subjects acting on behalf of the user].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [The security attributes of the connected session are not changed].

6.1.5 Security management class

FMT_MSA.1 (1) Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (1) The TSF shall enforce the [data access control SFP] to restrict the ability to *query, modify, delete and [add]* the security attributes on the [Table 17] to [U.ADMINISTRATOR].

FMT_MSA.1 (2) Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (2) The TSF shall enforce the [basic function access control SFP] to restrict the ability to *query and modify* the security attributes on the [Table 18]to [U.ADMINISTRATOR].

FMT_MSA.1 (3) Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 (3) The TSF shall enforce the [network information flow control security policy] to restrict the ability to *query, modify, delete and [add]* the security attributes of the [IP address and MAC address] to [U.ADMINISTRATOR].

FMT_MSA.3 (1) Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 (1) The TSF shall enforce the [data access control SFP] to provide the *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (1) The TSF shall allow the [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3 (2) Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 (2) The TSF shall enforce the [basic function access control SFP] to provide the *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (2) The TSF shall allow the [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3 (3) Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 (3) The TSF shall enforce the [network information flow control security policy] to provide the *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (3) The TSF shall allow the [U.ADMINISTRATOR] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to *query, modify, delete, [add, back up/restore]* the [the following list: Table 21] to [U.ADMINISTRATOR].

[Table 19] Management of TSF data

TSF data list	Query	Modify	Delete	Add	Back up/restore	User authority
Address book	O	O	O	O		U.USER (* U.NORMAL can modify, delete and register only his/her own address book)
User box setting	O	O	O	O		U.USER (* U.NORMAL can change, delete and register only the common box and his/her own box)
Work log, fax log	O	-	-	-	-	U.USER
Audit log	O	-	-	-	-	U.ADMINISTRATOR
User ID	O	O	-	-	-	
User password	-	O	-	-	-	
User authority (basic function)	O	O	-	-	-	
Security fax setting	O	O	-	-	-	
Network setting	O	O	-	-	-	
Security warning mail setting	O	O	O	O	-	
Mail server setting	O	O	O	O	-	
Address book Backup/ Restore	-	-	-	-	O	
SD Card setting(LUI)	O	O	-	-	-	
SSD setting(LUI)	O	O	-	-	-	
Service port	O	O	-	-	-	
IPSec setting	O	O	O	O	-	
SNMP setting	O	O	-	-	-	
login time limit	O	O	-	-	-	
Number of login attempts	O	O	-	-	-	
IP&MAC filtering setting	O	O	O	O	-	
Administrator connection IP setting	O	O	O	O	-	
Output authentication setting	O	O	-	-	-	
Fax data control setting	O	O	-	-	-	
MFP time setting	O	O	-	-	-	
Administrator box setting	O	O				
LDAP setting	O	O				
ID&Print setting	O	O				
User counter setting	O	O				
LDAP Address book setting	O	O				
SMB Kerberos setting	O	O				
Syslog setting	O	O				
IEEE802.1X setting	O	O				
Device Certificate setting (RUI)	O	O	O	O		
CA Certificate setting (RUI)	O	O	O	O		

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components

Dependencies: No dependencies

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [the following list: Table 22].

[Table 20] Management function

Management functions	Related SFR
Viewing audit log	FAU_SAR.1 FAU_SAR.2 FAU_SAR.3
Management of security attributes	FMT_MSA.1(1) FMT_MSA.1(2) FMT_MSA.1(3) FMT_MSA.3(1) FMT_MSA.3(2) FMT_MSA.3(3)
Management of TSF data	FMT_MTD.1

FMT_SMR.1 Security roles

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles: [U.ADMINISTRATOR, U.NORMAL].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 Protection of the TSF class

FPT_FDI_EXP.1 Restricted forwarding of data to external interfaces

Hierarchical to: No other components

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security roles

FPT_FDI_EXP.1.1 The TSF shall provide the capability to restrict data received on [any external interface] from being forwarded without further processing by the TSF to [any Shared-medium interface].

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components

Dependencies: No dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TST.1 TSF testing

Hierarchical to: No other components

Dependencies: No dependencies

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial startup, periodically during normal operations and at the request of authorized users* to demonstrate the correct operation of *[MFP Controller Software]*.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *[Encryption Key Data]*.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of *[Stored TSF executable code]*.

6.1.7 TOE access class

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after [between 60 seconds, specified by the administrator, and 600 seconds. The default value is 60 seconds].

6.1.8 Trusted path/channel class

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components

Dependencies: No dependencies

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the TSF and another trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [communication with trusted IT products].

6.2 Security Assurance Requirements

The security assurance requirements of this security target consist of the assurance components of Common Criteria Part 3 (CCMB-2012-09-003), and the evaluation assurance level is EAL2

6.2.1 Security Target evaluation class

ASE_INT.1 ST introduction

Dependencies: No dependencies

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview, and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies: ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

ASE_SPD.1 Security problem definition

Dependencies: No dependencies

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.2 Security objectives

Dependencies: ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.2 Derived security requirements

Dependencies: ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies: ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide TOE summary specification.

Content and presentation elements:

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification are consistent with the TOE overview and the TOE description.

6.2.2 Development class

ADV_ARC.1 Security architecture description

Dependencies: ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2 Security-enforcing functional specification

Dependencies: ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specifications to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 Basic design

Dependencies: ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall provide the behavior summary of each SFR-supporting or SFR non-interfering TSF subsystem.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.

Evaluator action elements:

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

6.2.3 Guidance documents Class

AGD_OPE.1 Operational user guidance

Dependencies: ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event related to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operations.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparation procedures to confirm that the TOE can be prepared securely for operations.

6.2.4 Life-cycle support class

ALC_CMC.2 Use of a CM system

Dependencies: ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements

for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of TOE or parts of it to the consumer.

ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.5 Tests class

ATE_COV.1 Evidence of coverage

Dependencies: ADV_FSP.2 Security-enforcing functional specification

ATE_FUN.1 function testing

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies: ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Dependencies: ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability analysis class

AVA_VAN.2 Vulnerability analysis

Dependencies: ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing the Basic attack potential.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements Rationale

[Table 21] Security Functional Requirements Rationale

security objectives / security functional requirements	O.DOC.NO_DIS	O.DOC.NO_ALT	O.FUNC.NO_ALT	O.PROT.NO_ALT	O.CONF.NO_DIS	O.CONF.NO_ALT	O.USER.AUTHORIZED	O.INTERFACE.MANAGED	O.SOFTWARE.VERIFIED	O.AUDIT.LOGGED
FAU_ARP.1										O

FAU_GEN.1										O
FAU_GEN.2										O
FAU_SAA.1										O
FAU_SAR.1										O
FAU_SAR.2										O
FAU_SAR.3										O
FAU_STG.1										O
FAU_STG.4										O
FCS_CKM.1(1)	O	O	O							
FCS_CKM.1(2)				O	O	O				
FCS_CKM.4	O	O	O							
FCS_COP.1	O	O	O	O	O	O				
FDP_ACC.1(1)	O	O	O							
FDP_ACC.1(2)							O			
FDP_ACF.1(1)	O	O	O							
FDP_ACF.1(2)							O			
FDP_IFC.2								O		
FDP_IFF.1								O		
FDP_RIP.1	O									
FIA_AFL.1(1)							O			
FIA_AFL.1(2)							O			
FIA_ATD.1							O			
FIA_UAU.1							O	O		
FIA_UAU.7							O			
FIA_UID.1	O	O	O	O	O	O	O	O		O
FIA_USB.1							O			
FMT_MSA.1(1)	O	O	O							
FMT_MSA.1(2)							O			
FMT_MSA.1(3)								O		
FMT_MSA.3(1)	O	O	O							
FMT_MSA.3(2)							O			
FMT_MSA.3(3)								O		
FMT_MTD.1				O	O	O				
FMT_SMF.1	O	O	O	O	O	O				
FMT_SMR.1	O	O	O	O	O	O	O			
FPT_FDI_EXP.1								O		
FPT_STM.1										O
FPT_TST.1									O	
FTA_SSL.3								O		
FTP_ITC.1	O	O	O	O	O	O				

[Table 22] Security Functional Requirements Rationale

Security Objectives	SFR	Rationale
O.DOC.NO_DIS	FCS_CKM.1(1)	Supports cryptographic operations when it is requested that the key for encrypting the user data repository should be generated
	FCS_CKM.4	Supports cryptographic operations when it is required that the key for the user data repository encryption should be destroyed
	FCS_COP.1	Enforces protection when cryptographic operations for the user data repository encryption is required
	FDP_ACC.1(1)	Enforces protection for establishing the access control policy
	FDP_ACF.1(1)	Supports the access control policy by providing the access control function

	FDP_RIP.1	Enforces protection by making residual data unavailable
	FIA_UID.1	Supports the access control and security role when user identification is required
	FMT_MSA.1(1)	Supports the access control function by controlling security attributes
	FMT_MSA.3(1)	Supports the access control function by controlling the default values of security attributes
	FMT_SMF.1	Supports control of security attributes when the attribute control function is required
	FMT_SMR.1	Supports control of security attributes when security roles are required
	FTP_ITC.1	Enforces protection by requesting the use of trusted channels for data communication through the SMI
O.DOC.NO_ALT	FCS_CKM.1(1)	Supports cryptographic operations when it is required that the key for the user data repository encryption should be generated
	FCS_CKM.4	Supports cryptographic operations when it is required that the key for the user data repository encryption should be destroyed
	FCS_COP.1	Enforces protection when cryptographic operations are required for the user data repository encryption
	FDP_ACC.1(1)	Enforces protection by establishing the access control policy
	FDP_ACF.1(1)	Supports the access control policy by providing the access control function
	FIA_UID.1	Supports the access control and security roles when user identification is required
	FMT_MSA.1(1)	Supports the access control function by controlling security attributes
	FMT_MSA.3(1)	Supports the access control function by controlling the default values of security attributes
	FMT_SMF.1	Supports control of security attributes when the attribute control function is required
	FMT_SMR.1	Supports control of security attributes when security roles are required
	FTP_ITC.1	Enforces protection by requesting the use of trusted channels for data communication through SMI
O.FUNC.NO_ALT	FCS_CKM.1(1)	Supports cryptographic operations when it is required that the key for the user data repository encryption should be generated
	FCS_CKM.4	Supports cryptographic operations when it is required that the key for the user data repository encryption should be destroyed
	FCS_COP.1	Enforces protection when cryptographic operations are required for the user data repository encryption
	FDP_ACC.1(1)	Enforces protection by establishing the access control policy
	FDP_ACF.1(1)	Supports the access control policy by providing the access control function
	FIA_UID.1	Supports the access control and security roles when user identification is required

	FMT_MSA.1(1)	Supports the access control function by controlling security attributes
	FMT_MSA.3(1)	Supports the access control function by controlling the default values of security attributes
	FMT_SMF.1	Supports control of security attributes when the attribute control function is required
	FMT_SMR.1	Supports control of security attributes when security roles are required
	FTP_ITC.1	Enforces protection by requesting the use of trusted channels for data communication through SMI
O.PROT.NO_ALT	FCS_CKM.1(2)	Supports cryptographic operations when it is required that the key for encryption of the user data repository should be generated
	FCS_COP.1	Supports cryptographic operations when it is required that the key for encrypting the user data repository should be destroyed
	FIA_UID.1	Enforces protection when cryptographic operations for encrypting the user data repository is required
	FMT_MTD.1	Enforces protection by establishing the access control policy
	FMT_SMF.1	Supports the access control policy by providing the access control function
	FMT_SMR.1	Supports the access control and security roles when user identification is required
	FTP_ITC.1	Supports the access control function by controlling security attributes
O.CONF.NO_DIS	FCS_CKM.1(2)	Supports cryptographic operations when it is required that the key for encrypting the address book backup/restore function should be generated
	FCS_COP.1	Supports the access control and security roles when user identification is required
	FIA_UID.1	Enforces the protection function by restricting access
	FMT_MTD.1	Supports control of security attributes when the attribute control function is required
	FMT_SMF.1	Supports control of security attributes when security roles are required
	FMT_SMR.1	Enforces protection by requesting the use of trusted channels for data communication through SMI
	FTP_ITC.1	Supports cryptographic operations when it is required that the key for encrypting the address book backup/restore function should be generated
O.CONF.NO_ALT	FCS_CKM.1(2)	Supports cryptographic operations when it is required that the key for encrypting the address book backup/restore function should be generated
	FCS_COP.1	Supports the access control and security roles when user identification is required
	FIA_UID.1	Enforces the protection function by restricting access
	FMT_MTD.1	Supports control of security attributes when the attribute control function is required

	FMT_SMF.1	Supports control of security attributes when security roles are required
	FMT_SMR.1	Enforces protection by requesting the use of trusted channels for data communication through SMI
	FTP_ITC.1	Supports cryptographic operations when it is required that the key for encrypting the address book backup/restore function should be generated
O.USER.AUTHORIZED	FDP_ACC.1(2)	Enforces authentication by establishing the access control policy
	FDP_ACF.1(2)	Supports the access control policy by providing the access control function
	FIA_AFL.1(1)	Delays authentication when authentication fails (U.ADMINISTRATOR)
	FIA_AFL.1(2)	Prevents authentication when authentication fails (U.NORMALAD)
	FIA_ATD.1	Supports authentication in connection with user security attributes
	FIA_UAU.1	Enforces authentication with user authentication
	FIA_UAU.7	Supports authentication by protecting authentication information feedback
	FIA_UID.1	Enforces authentication when user identification is required
	FIA_USB.1	Enforces authentication by classifying subject security attributes linked to user roles
	FMT_MSA.1(2)	Supports the access control function by controlling security attributes
	FMT_MSA.3(2)	Supports the access control function by controlling the default values of security attributes
	FMT_SMR.1	Supports control of security attributes when security roles are required
O.INTERFACE.MANAGED	FDP_IFC.2	Manages by establishing the network information flow control policy
	FDP_IFF.1	Supports the network information flow control policy by providing the information flow control function
	FIA_UAU.1	Enforces authentication with user authentication
	FIA_UID.1	Enforces authentication when user identification is required
	FMT_MSA.1(3)	Supports the information flow control function by controlling security attributes
	FMT_MSA.3(3)	Supports the information flow control function by controlling the default values of security attributes
	FPT_FDI_EXP.1	Enforces the function to restrict the direct forwarding of data from one external interface to another
	FTA_SSL.3	Enforces authentication when the termination of an inactive session is required
O.SOFTWARE.VERIFIED	FPT_TST.1	Enforces software verification when self-test is required
O.AUDIT.LOGGED	FAU_ARP.1	Enforces a security warning in case of security breaches

	FAU_GEN.1	Enforces the audit record policy when audit logs are required in relation to MFP functions
	FAU_GEN.2	Supports the security audit policy when the audit logs of information linked to logged events are generated
	FAU_SAA.1	Provides support when analysis of logged security audits is required
	FAU_SAR.1	Enforces restriction of the viewing of stored audit records to U.ADMINISTRATOR
	FAU_SAR.2	Prohibits all users from reading audit records except for those users who are clearly allowed to read
	FAU_SAR.3	Enforces application when the viewing of stored audit records according to the standard of logical relationship is required
	FAU_STG.1	Enforces protection of the audit records repository by preventing unauthorized alteration of stored audit records
	FAU_STG.4	Enforces protection of audit data from loss by overwriting oldest audit records
	FIA_UID.1	Enforces authentication when user identification is required
	FPT_STM.1	Supports the security audit policy by providing a correct time stamp when audit records are created

6.3.2 Security Assurance Requirements Rationale

This security target was developed in consideration of the assumption that it is operated in a limited environment where the level of document security and operational responsibilities require a relatively high level of assurance. The TOE was developed in consideration of the fact that it is operated in a physically secure environment and unauthorized access over the network is limited. User data is encrypted and stored in the SD card or SSD inside the MFP. The SD and SSD are inaccessible unless they are physically separated from the MFP. So user data is safe from the physical disclosure. Also, the self-verification function for executable codes is provided so that the malfunctions of the MFP can be detected. Accordingly, the Evaluation Assurance Level 2 is appropriate.

6.3.3 Dependency Rationale

[Table 23] Security Functional Requirements Rationale

No.	SFR	Dependencies	Satisfaction
1	FAU_ARP.1	FAU_SAA.1	4
2	FAU_GEN.1	FPT_STM.1	37
3	FAU_GEN.2	FAU_GEN.1 FIA_UID.1	2 26
4	FAU_SAA.1	FAU_GEN.1	2
5	FAU_SAR.1	FAU_GEN.1	2
6	FAU_SAR.2	FAU_SAR.1	5
7	FAU_SAR.3	FAU_SAR.1	5
8	FAU_STG.1	FAU_GEN.1	2
9	FAU_STG.4	FAU_STG.1	8
10	FCS_CKM.1(1)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	12 or 13

			11
11	FCS_CKM.1(2)	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4	Not satisfied (As the cryptographic key for the address book backup/restore function is generated by user input during every backup or restore, but is not stored in the system, key destruction is not necessary.)
12	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	10
13	FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 FCS_CKM.4	10 12
14	FDP_ACC.1(1)	FDP_ACF.1(1)	16
15	FDP_ACC.1(2)	FDP_ACF.1(2)	17
16	FDP_ACF.1(1)	FDP_ACC.1(1) FMT_MSA.3(1)	14 31
17	FDP_ACF.1(2)	FDP_ACC.1(2) FMT_MSA.3(2)	15 32
18	FDP_IFC.2	FDP_IFF.1	19
19	FDP_IFF.1	FDP_IFC.1 FMT_MSA.3(3)	18 33
20	FDP_RIP.1	-	-
21	FIA_AFL.1(1)	FIA_UAU.1	24
22	FIA_AFL.1(2)	FIA_UAU.1	24
23	FIA_ATD.1	-	-
24	FIA_UAU.1	FIA_UID.1	26
25	FIA_UAU.7	FIA_UAU.1	24
26	FIA_UID.1	-	-
27	FIA_USB.1	FIA_ATD.1	23
28	FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	14 35 36
29	FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	14 35 36
30	FMT_MSA.1(3)	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	18 35 36
31	FMT_MSA.3(1)	FMT_MSA.1(1) FMT_SMR.1	28 36
32	FMT_MSA.3(2)	FMT_MSA.1(2) FMT_SMR.1	29 36
33	FMT_MSA.3(3)	FMT_MSA.1(3) FMT_SMR.1	30 36
34	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	35 36
35	FMT_SMF.1	-	-
36	FMT_SMR.1	FIA_UID.1	26
37	FPT_STM.1	-	-
38	FPT_TST.1	-	-
39	FTA_SSL.3	-	-
40	FTP_ITC.1	-	-
41	FPT_FDI_EXP.1	FMT_SMF.1 FMT_SMR.1	35 36

[Table 24] Security Assurance Requirements Rationale

No.	SAR	Dependencies	Satisfaction
1	ADV_ARC.1	ADV_FSP.1 ADV_TDS.1	2 3
2	ADV_FSP.2	ADV_TDS.1	3

3	ADV_TDS.1	ADV_FSP.2	2
4	AGD_OPE.1	ADV_FSP.1	2
5	AGD_PRE.1	-	
6	ALC_CMC.2	ALC_CMS.1	7
7	ALC_CMS.2	-	
8	ALC_DEL.1	-	
9	ASE_INT.1	-	
10	ASE_CCL.1	ASE_INT.1 ASE_ECD.1 ASE_REQ.1	9 11 13
11	ASE_ECD.1		
12	ASE_OBJ.2	ASE_SPD.1	14
13	ASE_REQ.2	ASE_OBJ.2 ASE_ECD.1	12 11
14	ASE_SPD.1	-	
15	ASE_TSS.1	ASE_INT.1 ASE_REQ.1 ADV_FSP.1	9 13 2
16	ATE_COV.1	ADV_FSP.2 ATE_FUN.1	2 17
17	ATE_FUN.1	ATE_COV.1	16
18	ATE_IND.2	ADV_FSP.2 AGD_OPE.1 AGD_PRE.1 ATE_COV.1 ATE_FUN.1	2 4 5 16 17
19	AVA_VAN.2	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1 AGD_OPE.1 AGD_PRE.1	1 2 3 4 5

7. TOE Summary Specifications

7.1 TOE Security Functions

This section describes the security functions performed by the TOE to meet the security functional requirements described in Section 6.1.

7.1.1 Identification and Authentication Function

The TSF provides the function for identifying and authenticating users (U.USER). The administrator (U.ADMISTRATOR) uses the browser installed on the client computer through network connection to perform TOE security management, or uses the operation panel of the TOE to perform security management. Normal users (U.NORMAL) can use the operation panel of the TOE to use the functions provided by the TOE. If the administrator accesses the TOE for security management, the TOE identifies and authenticates the administrator so that the authorized administrator can perform security management. If the user accesses the TOE, the TOE identifies and authenticates the user so that the functions of the TOE are provided to the authorized user. The user identification and authentication mechanism is provided using the general ID/password method. It is possible to manage passwords by setting the following combination rule.

Combination rule: A combination of English alphabets, numbers and special characters
Password length: Minimum input (9~15 characters), maximum input (30 characters), default

setting 9 digits

For administrators, the combination rule must be included unconditionally, and for users, passwords can be managed according to the rule set by the administrator.

If a user fails to be authenticated as often as the number of times specified by the administrator, authentication will be restricted according to the following authentication failure policies.

> Administrator: Authentication is delayed for a certain amount of time specified by the administrator.
> Normal user: Authentication is prevented until the administrator allows it.

By default, up to five user failures are allowed, and the administrator may define the number of failures with an integer between 3 and 10.

When accessing the TOE through the RUI, users may use such functions as using menus unrelated to security (viewing product information, address book, and product status information) before identification and authentication.

While users are entering identification and authentication information, authentication information will be masked with * so that authentication feedback information can be protected.

According to the administrator's authentication setting, it operates in 3 modes, i.e. user authentication for individual users, group authentication for group users, and user authentication+group authentication. For user authentication and group authentication, identification and authentication operation is performed once, and if user authentication and group authentication are set as 'Yes' at the same time, identification and authentication operation is performed twice. That is, if authentication succeeds after user authentication, group authentication will be performed. If the administrator sets the "user/group interlock" as 'Yes', however, it operates only when user authentication succeeds.

7.1.2 Access control

The TSF protects user data by controlling access to user data while users are using the MFP. For the user data created by print, scan, and fax functions, the TOE denies accesses of all users excluding document owners by controlling those users who can access the user data based on the user ID. When logged in to the TOE through LUI, normal users can view or print out the list of the print data they own, and they also can forward scan data of their choice to external entities (USB, email, SMB, WebDAV, FTP), or store the scan data in the repository in the machine. When logged in to the TOE through LUI, administrators can view or print out the list of fax data. Only the owner of print, scan, fax functions can delete user data or jobs. There is no access restriction on the copy function.

The TSF controls access based on user ID and user's role with regard to using the basic functions of the MFP. When logged in to the TOE through LUI, normal users can only execute the functions that are allowed by the administrator (print, scan, copy, and fax).

The TSF provides the information flow control function based on the IP or MAC of the external IT entity. The administrator can control external IT entities, accessing the TOE over the network, based on information flow control security policy setting.

7.1.3 Security Audit

Audit logs are generated and stored when the MFP boots up and shuts down, and when related events listed in [Table 25] below occur.

[Table 25] Auditable events

SFR-related Auditable events	Details of auditable events	Related SFR
Audit records repository saturation	History of audit log repository saturation	FAU_STG.4
Response to administrator/user authentication failures	History of responses to authentication failures	FIA_AFL.1
Administrator/user authentication success/failure	History of authentication success/failure	FIA_UAU.1
Changes in data access control setting	History of changes in data access control setting	FMT_MSA.1(1)
Changes in basic function access control setting	History of changes in basic function access control setting change	FMT_MSA.1(2)
Network information flow control setting change	History of network information flow control setting change	FMT_MSA.1(3)
Data access control setting change	History of data access control setting change	FMT_MSA.3(1)
Basic function access control setting change	History of basic function access control setting change	FMT_MSA.3(2)
Network information flow control setting change	History of network information flow control setting change	FMT_MSA.3(3)
Security management result	History of administrator's security management excluding queries	FMT_MTD.1
Self-test result	Self-test result (success/failure)	FPT_TST.1
Session end result	Session termination result	FTA_SSL.3
Auditable events related to basic functions	**Details of auditable events**	**Remarks**
copy	Copy records	Auditable events of basic functions that are not related to SFR
scan	Scan records	
fax	Fax send/receive records	
print	Print records	

The TSF records event dates using the time stamp provided by the MFP when generating audit logs, and records information on event types, subject's identity and event results (success or failure).

The TSF provides the capability to detect potential violations, such as the administrator's consecutive authentication failures, audit log repository saturation, and errors during self-tests based on the stored audit data. If there are potential errors, the TSF uses e-mail to send a warning to help the administrator operate TSF stably.

The audit log created by TSF can be viewed and managed only by the administrator through the operation panel. The work log (Print, Scan and Copy history) and fax log (Fax history) can be viewed by the administrator and normal users through the operation panel.

When looking up the created audit data, the TSF can look up the auditable events by user ID.

It protects the audit records stored in the audit trail from unauthorized deletion, and prevents unauthorized alterations.

If the audit data repository is full, the TSF continuously stores the latest audit history by overwriting the oldest audit data first.

7.1.4 Security Management

The TSF provides the function to manage the TSF data defined in the [Table 28], which is used in the access control policy, to the identified and authenticated administrator.

[Table 26] TSF data management

TSF data list	Inquiry	Modify	Deletion	Addition	Backup/restore	User authority
Address book	O	O	O	O		User (* Normal users can modify, delete and register only the address book they own)
User box setting	O	O	O	O		user (* Normal users can change, delete and register only the common box and the box they own)
Work log, fax log	O	-	-	-	-	User
Audit log	O	-	-	-	-	Administrator
User ID	O	O	-	-	-	
User password	-	O	-	-	-	
User authority (basic function)	O	O	-	-	-	
Security fax setting	O	O	-	-	-	
Network setting	O	O	-	-	-	
Security warning mail setting	O	O	O	O	-	
Mail server setting	O	O	O	O	-	
Address book backup/restore	-	-	-	-	O	
SD Card setting (LUI)	O	O	-	-	-	
SSD setting (LUI)	O	O	-	-	-	
Service port (HTTP)	O	O	-	-	-	
IPSec setting	O	O	O	O	-	
SNMP setting	O	O	-	-	-	
login limit time	O	O	-	-	-	
Number of login attempts	O	O	-	-	-	
IP&MAC filtering setting	O	O	O	O	-	
Administrator connection IP setting	O	O	O	O	-	
print out authentication setting	O	O	-	-	-	
Fax data control setting	O	O	-	-	-	
MFP time setting	O	O	-	-	-	
Administrator box setting	O	O				
LDAP setting	O	O				
ID&Print setting	O	O				
User counter setting	O	O				
LDAP Address book setting	O	O				
SMB Kerberos setting	O	O				
Syslog setting	O	O				
IEEE802.1X setting	O	O				
Device Certificate setting (RUI)	O	O	O	O		
CA Certificate setting (RUI)	O	O	O	O		

The administrator can perform security management on the web through the operation panel of the MFP. The administrator must check the details of the security warning sent by the TSF via e-mail, and perform security management so that the TSF is always secure. To protect the address book data when

performing the address book backup/restore functions, the TSF provides the function to encrypt the address book. The cryptographic algorithm used for encryption is the AES block cryptographic algorithm, and 256-bit cryptographic keys are used. When generating the cryptographic key used for encrypting the address book, the TSF uses the Password Based Key Derivation Function (PBKDF1) to generate the cryptographic key when generating the cryptographic keys used for encrypting the address book. The cryptographic key for the address book backup/restore functions is generated by user input at every backup or restore, and it is not stored in the system

If the administrator manages the TOE via web (RUI) or operation panel (LUI), the TSF controls the session. If in the case of the web (RUI), the administrator does not do anything after login, the TSF provides the capability to terminate the session. Or if in the case of the operation panel (LUI), the user does not do anything after login, the TSF provides the capability to terminate the session. By default, the session is terminated after 60 seconds, and the value can be any number between 60 seconds and 600 seconds depending on the setting made by the administrator.

7.1.5 Stored Data Protection

The TSF provides the capability to protect user data stored in the TOE. The image data generated by the fax / scan jobs and the documents in the form of electronic files stored by the normal user for printing will be stored in the user data repository installed in the TOE (SD Card or SSD).

The TSF provides the capability to encrypt the data repository to protect stored user data. The cryptographic algorithm used for encryption is the AES block cryptographic algorithm. The AES cryptographic algorithm uses 256-bit cryptographic keys.

The TSF uses the Sindoh data repository cryptographic key generation algorithm to generate cryptographic keys when generating the cryptographic keys used for encryption. The generated cryptographic keys will be stored in the secure repository of the device. When the cryptographic key is destroyed, it is overwritten with ‘0’.

The TSF provides the function to delete the data stored in the user data repository. As the user data repository is installed physically inside the TOE, it is impossible to take the data repository out without permission. If the product is replaced or put into disuse, however, the data in the data repository must be deleted. At this time, the TSF deletes all domains of the data repository (overwriting them with ‘0’). Also, the TSF destroys the cryptographic keys used for encryption by overwriting them with ‘0’ when deleting all domains of the user data repository.

7.1.6 Self-protection

The TOE performs self-tests on a subset of the TSF to demonstrate correct operations of the TSF. The self-test is done at TOE start-up and regularly during the operation at the request of the administrator. TOE conducts self-tests when it starts periodically during regular operations and at the request of the administrator. The following TSFs are subject to self-tests.

Also, the TSF provides the capability to check the integrity of a subset of the TSF data (Encryption Key Data) and executable code. To check integrity, SHA256 hash algorithm is used. The hash values from the data saved at initial installation and the data saved by an on-demand integrity check are compared for integrity check. If the integrity of the TSF data is found compromised, the issue is reported to the administrator by an email, and an audit result is logged.

7.1.7 Fax Data Control

The TOE restricts data forwarding to external interfaces. The TOE restricts the forwarding of inbound fax data over PSTN to external interfaces. Direct data forwarding from PSTN to other interfaces is possible only in case where it is explicitly allowed by authorized administrative roles. All inbound data from external interfaces, excluding the fax data, is not allowed to be forwarded to any other external interface.

7.1.8 Trusted channel

The TSF provides encrypted communication listed in the [Table 29] below to ensure the security of the transmitted data during communication between the TOE and external IT entities (Client Computer, FTP server, WebDAV server, SMB server, Mail server, LDAP server, Kerberos server, Syslog server).

[Table 27] Encrypted Communication Provided by TOE

External IT entity	Encrypted Communication Provided by TOE	
	Protocol	**Encryption algorithm**
Client Computer	IPSec	AES(128bits), 3DES(168bits)
	TLS 1.2, TLS 1.3	AES(128bits, 192bits, 256bits), 3DES(168bits)
FTP server	IPSec	AES(128bits), 3DES(168bits)
	TLS 1.2, TLS1.3	AES(128bits, 192bits, 256bits), 3DES(168bits)
WebDAV server	IPSec	AES(128bits), 3DES(168bits)
	TLS 1.2, TLS1.3	AES(128bits, 192bit, 256bits), 3DES(168bits)
SMB server	IPSec	AES(128bits), 3DES(168bits)
Mail server	IPSec	AES(128bits), 3DES(168bits)
	TLS 1.2, TLS1.3	AES(128bits, 192bits, 256bits), 3DES(168bits)
LDAP server	IPSec	AES(128bits), 3DES(168bits)
Kerberos server	IPSec	AES(128bits), 3DES(168bits)
Syslog server	IPSec	AES(128bits), 3DES(168Bits)